POLICY OR PRECEDENT

SUBJECT: DATE: 14 May 2008

Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII)

POLICY NUMBER	ORIGINATING SECTION	ORIGINATOR	PHONE #
16-08	AOIM-ISM	Ms. Bowling	432-9233

//Original Signed//
APPROVED BY: ROBERT W. WAGNER, LTG, USA, COMMANDING GENERAL

SYNOPSIS:

1. PURPOSE: To delineate the responsibility for safeguarding personally identifiable information created and maintained by the U.S. Army Special Operations Command (USASOC) and to establish reporting procedures for lost, stolen, or compromised PII.

2. SCOPE: This policy or precedent applies to all elements of Headquarters, USASOC, Major Subordinate Commands (MSCs), Major Subordinate Units (MSUs), Direct Reporting Units (DRUs), family members, contractors and their employees.

3. GENERAL:

a. The PII is defined as any information about an individual maintained by an agency, which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, and biometric records, etc., including any other personal information which is linked or linkable to an individual.

PRESCRIBING DIRECTIVE: Memorandum, Office of the Secretary of Defense, subject: Safeguarding Against and Responding to the Breach of Personally Identifiable Information, 21 Sep 07.

DISTRIBUTION:
This publication is available in electronic media and is intended for A5 distribution. Paper copies will be provided for those not having access to e-media.

OTHER POLICIES AFFECTED:
None.

b. All personnel, whether military, civilian or contractor, have an affirmative responsibility to ensure that personal and PII is collected, maintained, used, and disseminated only as authorized by law and regulation and that the information is continually safeguarded.

c. The safeguarding requirement includes any form of PII whether it be non-automated (verbal or paper) or data-at-rest (DAR). The DAR is defined as all data in computer storage, but excludes any data that frequently traverses the network or that which resides in temporary memory. The DAR includes, but is not limited to, archived data which is not accessed or changed frequently, files stored on hard drives, laptop computers, USB thumb drives; files stored on an external back up medium, and disks; and also files stored off-site or on a storage area network (SAN).

d. A loss or compromise occurs when personal information about an individual that would normally be withheld from the public is lost, stolen, shared or otherwise made known to another person who does not have a need to know the information in order to perform official duties.

e. All incidents of lost, stolen, or compromised information must be reported to the USASOC Freedom of Information Act/ Privacy Act (FOIA/PA) Office as soon as possible, preferably within one hour of discovery, to comply with statutory reporting requirements. The report must be submitted to the USASOC FOIA/ PA Office, at (910) 432-9233/9107. Incident Reports can also be emailed to: PA@soc.mil.

f. Enclosed is a sample of the format that may be used to report incidents to the FOIA/PA Office.

g. Incident reports must include: the organization involved, the date of the incident, the number of individuals impacted, a brief description of the incident (circumstances of the breach and the information lost or compromised), and point of contact information.

h. To ensure proper reporting to higher authorities, all incidents of lost, stolen or compromised DAR (such as laptop computers and thumb drives) must be reported to the USASOC FOIA/PA Officer even when there is no reason to believe PII has been compromised.

i. When an incident is reported, the FOIA/PA Office will vet the situation with all relevant USASOC subject matter experts (i.e., Information Assurance, Staff Judge Advocate, etc.). If it is verified that personally identifiable information within the command and control of a USASOC entity has been lost, stolen or compromised, the USASOC FOIA/PA Office will assist in the notification process. Affected parties will be notified as soon as possible, but not later than 10 working days from the date when the loss or compromise of personal information was discovered.

USASOC Incident Report
of Lost, Stolen, or Compromised
Personally Identifying Information

Incident:

a. **Component/Organization involved**. Sample: DOD-wide, including all services.

b. **Date of incident and the number of individuals impacted**. Sample: 5 April 2006; Approximate 14,000 active duty and retired service members and dependents.

c. **Brief description of incident; circumstances of the breach; information lost or compromised (if applicable)**. Sample: Hackers stole data from the DOD's TRICARE Management Activity system. Personally identifiable information (to include names, SSNs, credit card information, and other personal data) was potentially compromised.

d. **Point of Contact name, telephone number and email**. Sample: Mr. John Smith, (XXX) XXX-XXXX, john.smith@us.army.mil.